APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/773,057	01/30/2001	Rares Stefan	GO31-001	6026

			EXAMINER
25545	7590	06/07/2004	NALVEN, ANDREW L

GOUDREAU GAGE DUBUC
800 PLACE VICTORIA, SUITE 3400
MONTREAL, QUEBEC, H4Z 1E9
CANADA

ART UNIT	PAPER NUMBER
2134	

DATE MAILED: 06/07/2004

3

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)
	09/773,057	STEFAN, RARES
	Examiner	Art Unit
	Andrew L Nalven	2134

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE _3_ MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on _30 January 2001_.

2a)☐ This action is **FINAL.**   2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) _1-25_ is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) _1-25_ is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on _25 January 2001_ is/are: a)☒ accepted or b)☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☐ All   b)☐ Some * c)☐ None of:

      1.☐ Certified copies of the priority documents have been received.

      2.☐ Certified copies of the priority documents have been received in Application No. _____.

      3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _2_.

4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .

5) ☐ Notice of Informal Patent Application (PTO-152)

6) ☐ Other: _____.

DETAILED ACTION

1.   Claims 1-25 are pending.

2.   IDS submitted 5/10/01 has been received and considered.

Claim Rejections - 35 USC § 112

3.   The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

4.   Claim 1 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. Claim 1 provides the following limitation, "said back-end server being configured so as to prevent leaks from the network elements." The limitation amounts to a statement of the intended use of the system and thus fails to limit the scope of the claim to a particular structure (see MPEP 2106).

Claim Rejections - 35 USC § 102

5.   The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

6.   Claims 1-5, 9-10, and 25 are rejected under 35 U.S.C. 102(e) as being

anticipated by Epstein et al US Patent No 6,584,508. Epstein discloses an advanced

data guard having independently wrapped components.

7.   With regards to claim 1 (as best understood), Epstein teaches a front-end server

having internal and external interfaces (Epstein, Figure 5, column 9 lines 2-4, column 3

line 60 – column 4 line 5), the front-end server external interface being attached to the

public network (Epstein, Figure 5, column 9 lines 2-4), the front-end server being

configured to drop non-requested incoming packets from the public network (Epstein,

column 10 lines 7-15, column 9 lines 13-19), the non-requested packets including

signed packets and unsigned packets (Epstein, column 12 lines 53-58), a back-end

server having internal and external interfaces (Epstein, Figure 5, column 9 lines 1-2,

column 3 line 60 – column 4 line 5), the back-end internal interface being attached to

the network elements and to the front-end internal interface via the back-end external

interface (Epstein, Figure 5, column 9 lines 1-6), the back-end server being configured

to gather packets requested by the network elements from the public network and

signed packets from the front-end server (Epstein, column 9 lines 56-65), and the back-

end server being configured so as to prevent leaks from the network elements (Epstein,

column 10 lines 33-36).

8.   With regards to claim 2, Epstein teaches at least one of the front-end and back-

end servers being configured to implement IP filtering (Epstein, column 9 lines 49-55,

column 8 lines 25-35).

9.   With regards to claim 3, Epstein teaches the front-end and back-end servers

implement IP filtering according to the same rules (Epstein, column 9 lines 7-21, column

9 line 56 – column 10 line 6).

10.   With regards to claim 4, Epstein teaches the back-end server configured to   .

capture at least one request from one of the network elements and to analyze the

request for legitimacy before passing it to the public network (Epstein, column 9 line 56

– column 10 line 1).

11.   With regards to claim 5, Epstein teaches the back-end server being configured to

detect a transfer of data from the network elements to the public network (Epstein,

column 9 line 56 – column 10 line 1).

12.   With regards to claim 9, Epstein teaches the back-end server including an

application gateway (Epstein, column 3 lines 60-65, column 9 lines 1-6).

13.   With regards to claim 10, Epstein teaches the back-end server including a proxy

service (Epstein, column 3 lines 60-65, column 9 lines 1-6, Figure 5).

14.   With regards to claim 25, Epstein teaches the public network being the Internet

(Epstein, Figure 1).

Claim Rejections - 35 USC § 103

15.   The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set
> forth in section 102 of this title, if the differences between the subject matter sought to be patented and
> the prior art are such that the subject matter as a whole would have been obvious at the time the
> invention was made to a person having ordinary skill in the art to which said subject matter pertains.
> Patentability shall not be negatived by the manner in which the invention was made.

16.   Claim 6 is rejected under 35 U.S.C. 103(a) as being unpatentable over Epstein et al US Patent No 6,584,508.

17.   With regards to claim 6, Epstein teaches an interface between the front and back end servers but fails to specifically teach the interface using Ethernet cards. Examiner takes official notice that Ethernet cards are well known in the art and thus at the time the invention was made, it would have been obvious to a person of ordinary skill in the art to utilize Ethernet cards with Epstein's data guarding system because they provide a standard well known method of interfacing computers using the TCP/IP protocol that offers fast data transfer rates.

18.   Claim 7-8, 11-13, and 24 are rejected under 35 U.S.C. 103(a) as being unpatentable over Epstein et al US Patent No 6,584,508 in view of Antur et al US Patent No 6,212,558. Antur discloses a method and apparatus for reconfiguring and managing firewalls and security devices.

19.   With regards to claims 7-8, Epstein fails to teach the front-end server configured with a first OS and the back end server configured with a second OS. Antur teaches the front-end server configured with a first OS and the back end server configured with a second OS (Antur, column 10 lines 25-39, column 7 lines 28-44, Figure 4A). At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to utilize Antur's method of having different operating systems with Epstein's data guarding system because it offers the advantage of providing a more varied security

layout because the different operating systems provide different security capabilities

and provide the ability to support mixed protocol networks (Antur, column 1 lines 55-63).

20.   With regards to claim 11, Epstein fails to teach the front-end server being

configured to provide network address translation. Antur teaches a server being

configured to provide network address translation (Antur, column 4 lines 65-67). At the

time the invention was made, it would have been obvious to a person of ordinary skill in

the art to utilize Antur's method of having the firewall servers provide NAT with Epstein's

data guarding system because it offers the advantage of improving security by allowing

the masking of the real IP addresses of nodes on the internal network to ensure that the

nodes appear invisible to the outside (Antur, column 4 lines 65-67).

21.   With regards to claim 12, Epstein as modified teaches the NAT implemented to

not allow DNS (Antur, Figure 16).

22.   With regards to claim 13, Epstein fails to teach the front-end server having a third

interface. Antur discloses the front-end server having a third interface (Antur, Figure 2,

column 7 lines 22-26). At the time the invention was made, it would have been obvious

to a person of ordinary skill in the art to utilize Antur's method of having additional

network interfaces with Epstein's data guarding system because it offers the advantage

of providing the ability to implement security policy for a large number of servers (Antur,

column 2 lines 39-49, column 7 lines 22-26).

23.   With regards to claim 24, Epstein as modified teaches the front-end server

attached to the public network via a router (Antur, Figure 4(a)). At the time the invention

was made, it would have been obvious to a person of ordinary skill in the art to utilize

Antur's method of using routers with Epstein's data guarding system because routers offer the advantage of an inexpensive packet filtering firewall service (Antur, column 4 lines 29-40).

24.   Claim 14-16 are rejected under 35 U.S.C. 103(a) as being unpatentable over Epstein et al US Patent No 6,584,508 Antur et al US Patent No 6,212,558, as applied to claim 13 above, and in further view of Underwood US Patent No 6,523, 027.

25.   With regards to claims 14 and 16, Epstein as modified fails to teach at least one of a DNS server, a web server, an email server, and a time server connected to the third interface of the front-end server and the third interface configured so as to provide a DMZ for at least one of the DNS server, a web server, an email server, and a time server. Underwood teaches at least one of a DNS server, a web server, an email server, and a time server connected to the third interface of the front-end server and the third interface configured so as to provide a DMZ for at least one of the DNS server, a web server, an email server, push mail server, and a time server (Underwood, column 312 lines 30-38). At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to utilize Underwood's method of including servers in a DMZ with Epstein's modified data guarding system because it offers the advantage providing a higher level of performance and reliability (Underwood, column 312 lines 40-48).

26.   With regards to claim 15, Epstein as modified teaches the front-end server being configured to examine requests sent to one of the at least one DNS, web, email, and

time servers for potentially malicious commands (Underwood, column 312 lines 40-45, Epstein, column 9 lines 49-55).

27.   Claims 17-23 are rejected under 35 U.S.C. 103(a) as being unpatentable over Epstein et al US Patent No 6,584,508, Antur et al US Patent No 6,212,558, and Underwood US Patent No 6,523, 027, as applied to claim 13 above, and in further view of Kim et al US Patent No 6,701,440. Kim discloses a method and system for protecting a computer using a remote email-scanning device.

28.   With regards to claim 17, Epstein as modified fails to teach the transferring of email from a mail server to an internal mail server. Kim teaches the transferring of email from a mail server to an internal mail server (Kim, Figure 2). At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to utilize Kim's method of transferring emails from a server to an internal server with Epstein's modified data guarding system because it offers the advantage of being able to intercept and remove viruses or malicious code prior to the arrival of the message within a secure system (Kim, column 2 line 59 – column 3 line 3).

29.   With regards to claim 18-20, Epstein as modified fails to teach the push mail server being configured to verify email for malicious content or viruses and to remove the malicious content or viruses. Kim teaches the push mail server being configured to verify email for malicious content or viruses and to remove the malicious content or viruses (Kim, column 3 lines 19-44). At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to utilize Kim's method of

transferring emails from a server to an internal server with Epstein's modified data guarding system because it offers the advantage of being able to intercept and remove viruses or malicious code prior to the arrival of the message within a secure system (Kim, column 2 line 59 – column 3 line 3).

30.   With regards to claim 21, Epstein as modified teaches the inclusion of an internal site firewall attached to the internal interface of the back-end server with the internal mail server attached to the internal site firewall (Underwood, column 312 lines 30-38).

31.   With regards to claim 22-23, Epstein as modified teaches at least one of a DNS server, a web server, an email server, and a time server connected to the third interface of the front-end server and the third interface configured so as to provide a DMZ for at least one of the DNS server, a web server, an email server, push mail server, and a time server (Underwood, column 312 lines 30-38).

Conclusion

32.   The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

33.   Yarborough et al US Patent No 6,718,388 discloses a secured session sequencing proxy system and method therefore.

34.   Any inquiry concerning this communication or earlier communications from the examiner should be directed to Andrew L Nalven whose telephone number is 703 305

8407. The examiner can normally be reached on Monday - Thursday 8-6, Alternate

Fridays.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's

supervisor, Gregory Morse can be reached on 703 308 4789. The fax phone number

for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the

Patent Application Information Retrieval (PAIR) system. Status information for

published applications may be obtained from either Private PAIR or Public PAIR.

Status information for unpublished applications is available through Private PAIR only.

For more information about the PAIR system, see http://pair-direct.uspto.gov. Should

you have questions on access to the Private PAIR system, contact the Electronic

Business Center (EBC) at 866-217-9197 (toll-free).

Andrew Nalven

MATTHEW SMITHERS
PRIMARY EXAMINER
Art Unit 2137